insights

Volume: 25 Issue: 20

By: **Bev Townsend**

September 20, 2021

Decoding the Proposed European Union Artificial Intelligence Act

Introduction

Rapid advancement in the development and deployment of Artificial Intelligence (AI) holds unprecedented promise to transform the economy, business, healthcare, and society in general. As these developments escalate and deepen, interest in AI-associated rights and ethics is gaining ground. This is, in part, because AI technologies now harness vast quantities of personal data, myriad analytical and statistical tools, and tremendous computational power, and the effects on humanity's interests and well-being are uncertain.

The rise of AI presents newly-emergent legal and ethical challenges. Controversial technologies include facial recognition systems, computer sensors and vision, and autonomous vehicles (self-driving vehicles and care assistance robots, for instance). Specific concerns include data privacy, the prevalence and perpetuation of algorithmic injustice by and within the system, the unfair use of predictive models in decision-making, and the potential for the manipulative and malicious use of AI (amongst others). Policy and regulatory frameworks are now being developed to address these challenges. This *Insight* explores the major features of the recently proposed European Union Artificial Intelligence Act and how it seeks to protect and balance key values.

An Overview of Regulatory Options

Existing legal frameworks often fail to keep pace with emerging novel technologies. A published report by Cognilytica on Worldwide AI Laws and Regulations demonstrates that many countries are adopting a "wait and see" approach to AI regulatory implementation.[1] But, while most countries may still have very few or no *sui generis* AI

laws and regulations, a proliferation of international and sector-specific voluntary ethics standards and guidelines have been issued. These include efforts and proposals by UNESCO,[2] IEEE,[3] ISO,[4] Google,[5] and Microsoft,[6] to name but a few. Such efforts, however, serve pointedly to demonstrate the comparative lack of available hard law and governance around the world. Many of these ethical instruments contain shared, aspirational, "high-level" principles, which, although helpful, are largely formulaic in nature and are often sector or industry specific and not always easily operationalized. Certain more recent guidelines such as the Council of Europe's Guidelines on facial recognition, for instance, provide specific guidance on a narrow aspect of new AI technology adoption.[7]

However, the regulatory lag is closing—and closing rapidly. Emerging data-driven and AI technology-based regulations are now being noted. Broadly, we can identify three different approaches to AI-related regulation. First is regulating a particular aspect of AI technology—such as the data—as found in various data privacy laws. Safeguarding data, and particularly personal data, by means of legislative measures is now increasingly widespread. AI is inextricably linked to data, and thus impacted directly by data privacy laws. To date a total of 145 jurisdictions worldwide have data privacy and protection laws of one sort or another.[8] One of the most recent is The Personal Information Protection Law of the People's Republic of China, anticipated to take effect in November 2021. Thirteen new data privacy laws were enacted in 2019-2020 including the *California Privacy Rights Act of 2020*, the *Kenya Data Protection Act, 2019* and the *Barbados Data Protection Act, 2019*. Perhaps surprisingly, seven of the 13 new data privacy laws emanate from Africa (with 32 African countries in total having enacted data protection laws), making it the fastest expanding region.[9]

The second approach to regulation is to target a particular mischief in AI technology, such as the malicious or predatory use of AI technologies within a particular context. This approach was demonstrated in late August 2021 by the Cyberspace Administration of China's release of its pioneering draft Algorithm Regulations.[10] These regulations are a consequence of the increasing commercial deployment of AI and data-driven algorithms in the region. Provisions of the regulations focus primarily on empowering customers and protecting customers' rights by curbing predatory digital business practices, exploitative data usage, and unwanted intrusions into online activities.

The third approach is the one adopted by the EU. This approach provides horizontal regulation of AI systems that is distinctively broader, bolder, and more value-laden. But the adoption of such an approach comes with risk: in covering too much ground, certain

aspects of the legislation can slip into conceptual and procedural vagueness. Some of the more salient features of this proposed legislation are set out below.

The Proposed Regulation Laying Down Harmonised Rules on Artificial Intelligence

On April 21, 2021, the European Commission published the highly anticipated proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (AI Act or the Act).[11] This followed the Commission's ongoing commitment to establish "legislation for a coordinated European approach on the human and ethical implications of AI."[12] At the outset it is worth noting that, rather than focusing on the properties or outcomes of AI, the Act defines an "AI system" as software that is developed using certain *techniques and approaches* (detailed in an annex) that can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.[13] Any AI system developed not using one of the enumerated techniques or approaches falls outside of the definition—a definition that, because of its imprecision, creates the opportunity to skilfully circumvent the Act.

The intention is for the new legal framework to provide a set of harmonised rules that align (and are consistent with) existing EU human rights instruments and EU law regulating data protection, data governance, consumer protection, non-discrimination, and gender equality. Accordingly, a cautious yet balanced and proportionate regulatory approach is proposed, one that is primarily risk-based. It sets out the minimum necessary requirements to address risks to values, fundamental rights, and principles associated with AI development and deployment without unnecessarily constraining technological development or trade.[14]

What the Act does—and does well—is to differentiate requirements by risk level and to prohibit more objectionable AI systems that carry what is considered "undesirable risk" of fundamental rights infringement. The Act also introduces new legal obligations (such as monitoring, reporting, and transparency obligations) to manage those systems that, although not prohibited, are considered high risk. Amongst others, the Act establishes a robust governance, monitoring, and enforcement regime, sets up a European Artificial Intelligence Board, and seeks to impose sanctions and penalties for non-compliance.

Adopting a Risk-Based Approach: The Level of Risk Determines the Applicable Rules

The central tenet of the AI Act is to introduce a set of binding rules based upon the intensity and scope of the risk generated by the AI system. The impetus for such a risk-driven approach is that persons at risk and vulnerable to health, safety, and rights

infringement by new AI technologies require a higher level of protection. This is premised on the understanding that AI systems have certain characteristics (inter alia, an opacity, complexity, dependency on data, and capacity for autonomous behaviour) that can adversely and significantly affect fundamental human rights—rights to data privacy, transparency, autonomy, and the like.[15]

The Act addresses three categories of risk:

1. Prohibited Systems. Prohibited systems include AI systems that manipulate human behavior and/or exploit persons' vulnerabilities; social scoring systems; and, save for certain exceptions, "real-time" and "remote" biometric identification (or facial recognition) systems.

2. High-Risk Systems. While not clearly defined, a "high-risk" system is understood to be one that poses significant risk to health, safety, and fundamental rights. Although the AI Act applies generally to all AI systems, certain provisions contained within the Act (and provided for in Title III) apply specifically to those considered high-risk.

High-risk systems are either those products (or safety components of products) already covered by EU health and safety harmonisation legislation (such as medical devices, toys, and machinery, for instance) or those AI systems used in specified areas and contained in an annex to the Act (such as educational training, employment, and law enforcement).[16] Rather than relying on certain criteria to position a system as high-risk, the Act designates as high-risk all AI systems used within a specified enlisted and pre-determined domain. There are also no gradations of high-risk systems—either a system is high-risk, in which case compliance with a comprehensive list of requirements and obligations is prescribed, or it is not.

Once it has been established that an AI system is high-risk, it is mandated that the system's provider (the person, agency, or body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark[17]) must fulfill certain requirements and obligations. These requirements include that quality and risk management systems be implemented; that training, validation, and testing datasets be subject to appropriate data governance and management practices and meet data quality criteria; that technical documentation be drawn up and proper records be kept; and that transparency obligations be fulfilled.[18] These obligations are set out in detail within the Act.

An important further requirement is that high-risk AI systems be designed and developed to allow for human oversight so that natural persons can oversee their functioning. Providers are required to introduce "human-machine interface tools" and measures to guarantee that a system is subject to built-in operational constraints that cannot be overridden by the system itself and is responsive only to a human operator.

3. Low- or Minimal-Risk Systems. All other AI systems that are without risk, or are of low or minimal risk, can be developed, sold, and deployed without additional legal obligations subject, of course, to compliance with any existing relevant legislation (including data protection legislation, such as the GDPR). Moreover, those that design and deploy low- or minimal-risk systems are encouraged to adhere to voluntary codes of conduct.

Disclosing Bots, Detecting Emotions, and Deep Fakes

Although there are no special requirements for low-risk systems, transparency obligations apply to *all* risk-levels, and three categories of disclosable activities are distinguished.

First, providers of AI systems must design systems so that natural persons are informed that they are interacting with an AI system (so-called robot or "bot" disclosures). This disclosure is to avoid any potential confusion by a natural person when interacting with an AI system. It is not necessary to make such a disclosure in instances where it is contextually obvious that persons are interacting with an AI system. Second, users of systems that detect emotions or determine association with (social) categories based on biometric data must be informed of the operation of the system except in instances permitted by law or in crime prevention. And lastly, although certain exemptions apply, it is required that creators of artificial images, video, or audio content disclose that they have been generated synthetically or manipulated, such as in the case of "deep fakes."[19]

Extraterritorial Reach

Crucially, if adopted in its proposed form, the AI Act, much like the GDPR, will be far-reaching and have significant consequences beyond the EU. The Act has extraterritorial effect and, subject to certain specific exceptions, applies to: (i) providers that place on the market or deploy AI systems in the EU, regardless of where such providers are located; (ii) users of AI systems located within the EU; and (iii) providers and users of AI systems that are located outside the EU to the extent that the output produced by the system is used within the EU.

Conclusion: A Step in the Right Direction

If the AI Act is strikingly similar to the GDPR, it is perhaps no coincidence. Is the AI Act likely to become the new global "gold standard" for the adoption of AI regulation? Will the EU be the sole and dominant crafters of the laws governing technology? Certainly, many low- and medium-resource countries look to regulations such as those promulgated by the EU to guide and inform their new regulatory policy development.

To this end, and despite various shortcomings, the Act is a valuable start in helping to shape global norms and standards and promote trustworthy AI—AI systems that are, at least to some degree, more consistent with human values and interests. The Act also promotes innovation, including regulatory sandboxes and specific measures to support small-scale users and providers. Some may say that in preserving rights it does not go far enough, while innovators and developers may argue that it goes too far. But promoting ethical innovation and fair competition while balancing rights is not easily done—compromise is often needed—and the right regulatory framework should (prudently) do both.

But by covering too much ground—fundamental rights, health and safety, data protection, and consumer law—there is a risk that the practical operationalisation and implementation of the law may be untenable. Further, a plausible framework should also be nuanced and flexible enough to adapt to, and keep abreast of, the rapidly evolving landscape that is AI development and deployment. Whether the AI Act does this sufficiently in its present form remains to be seen.

About the Author: Dr. Bev Townsend is a Research Associate at the University of York. Her research is the Law and Ethics of Resilient Autonomous Systems.

---

[1] Cognilytica Research. Worldwide AI Laws and Regulations 2020, https://www.cognilytica.com/2020/02/14/worldwide-ai-laws-and-regulations-2020/; *see also* Kathleen Walch, *AI Laws are Coming*, FORBES, (Feb. 20, 2020), https://www.forbes.com/sites/cognitiveworld/2020/02/20/ai-laws-are-coming/?sh=3f2cad98a2b4.

[2] Available at https://en.unesco.org/courier/2018-3/towards-global-code-ethics-artificial-intelligence-research.

[3] Available at https://www.ieee.org/about/corporate/governance/p7-8.html.

[4] Available at https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/codeethics_2004-en.pdf.

[5] Available at https://ai.google/principles/.

[6] Available at https://www.microsoft.com/en-us/ai/our-approach-to-ai.

[7] Council of Europe, Guidelines on facial recognition 2021, https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html.

[8] Graham Greenleaf, *Global Data Privacy Laws 2021: Despite COVID Delays*, *145 Laws Show GDPR Dominance*, 169 PRIVACY LAWS & BUSINESS INT'L REP., 1, 3-5,
SSRN: https://ssrn.com/abstract=3836348 or http://dx.doi.org/10.2139/ssrn.3836348.
[9] *Id.*
[10] Available at https://digichina.stanford.edu/news/translation-internet-information-service-algorithmic-recommendation-management-provisions.
[11] European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021) 206 final (Apr. 21, 2021), https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206 [hereinafter AI Act].
[12] Ursula von der Leyen, *A Union that Strives for More: My Agenda for Europe* (Political Guidelines for the Next European Commission 2019-2024, 2019).
[13] AI Act, art. 3(1).
[14] *Id.*, Explanatory Memorandum ¶ 3.5.
[15] *Id.*
[16] AI Act, arts. 6-7 and Annex III.
[17] *Id.* art. 3(2).
[18] *Id.* ch. 3, arts. 16-29.
[19] *Id.* art. 52.